Access Control Lists

Information About Access Control Lists

An Access Control List (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). After ACLs are configured on the controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

You may also want to create a preauthentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

Both IPv4 and IPv6 ACL are supported. IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

Note You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Restrictions on Access Control Lists

- You can define up to 64 ACLs, each with up to 64 rules (or filters) for both IPv4 and IPv6. Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet.
- When you apply CPU ACLs on a Cisco 5508 WLC or a Cisco WiSM2, you must permit traffic towards the virtual interface IP address for web authentication.
- All ACLs have an implicit “deny all rule” as the last rule. If a packet does not match any of the rules, it is dropped by the controller.
- If you are using an external web server with a Cisco 5508 WLC or a WLC network module, you must configure a preauthentication ACL on the WLAN for the external web server.
- If you apply an ACL to an interface or a WLAN, wireless throughput is degraded when downloading from a 1-Gbps file server. To improve throughput, remove the ACL from the interface or WLAN, move the ACL to a neighboring wired device with a policy rate-limiting restriction, or connect the file server using 100 Mbps rather than 1 Gbps.
- Multicast traffic received from wired networks that is destined to wireless clients is not processed by WLC ACLs. Multicast traffic initiated from wireless clients, destined to wired networks or other wireless clients on the same controller, is processed by WLC ACLs.
- ACLs are configured on the controller directly or configured through Cisco Prime Infrastructure templates. The ACL name must be unique.
- You can configure ACL per client (AAA overridden ACL) or on either an interface or a WLAN. The AAA overridden ACL has the highest priority. However, each interface, WLAN, or per client ACL configuration that you apply can override one another.
- If peer-to-peer blocking is enabled, traffic is blocked between peers even if the ACL allows traffic between them.
- Authentication traffic has to go through the Cisco WLC for this feature to be supported, even if DNS-based ACL is local to the AP.
- When you create an ACL, it is recommended to perform the two actions (create an ACL or ACL rule and apply the ACL or ACL rule) continuously either from CLI or GUI.
- In Cisco Wireless Releases prior to 8.0.100.0, the behavior of the Redirect-URL-ACL (as returned via RADIUS attributes) may have been incorrect. The ACL was applied in only the Ingress direction (traffic destined for the LAN or distribution system) of the radio interface. These ACLs should also be applied in the Egress direction (traffic destined for the wireless client). Therefore, after upgrading to a Cisco Wireless Release 8.0 or a later release, you may need to adjust the ACL to accommodate the correction of this behavior.
- Mobility pings on ports 16666 and 16667 are notable exemptions and these ports cannot be blocked by any ACL.

Note ACL ID 0 is not supported in Cisco WLC. Foreign WLC does not send url-redirect-acl to anchor WLC if the received ACL attribute from RADIUS/ISE is mapped to ACL ID 0. It causes web redirect failure on wireless client later.

Configuring and Applying Access Control Lists (GUI)

Configuring Access Control Lists

Step 1 Choose **Security** > **Access Control Lists** > **Access Control Lists** to open the Access Control Lists page.

Step 2 If you want to see if packets are hitting any of the ACLs configured on your controller, select the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unselected, which is the default value. This feature is useful when troubleshooting your system.

Note If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.

Step 3 Add a new ACL by clicking **New**. The Access Control Lists > New page appears.

Step 4 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type. There are two types of ACL supported, IPv4 and IPv6.

Step 6 Click **Apply**. When the Access Control Lists page reappears, click the name of the new ACL.

Step 7 When the Access Control Lists > Edit page appears, click **Add New Rule**. The Access Control Lists > Rules > New page appears.

Step 8 Configure a rule for this ACL as follows:

a) The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b) From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

- **Any—**Any source (this is the default value).
- **IP Address—**A specific source. If you choose this option, enter the IP address and netmask of the source in the text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

c) From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any—**Any destination (this is the default value).

- **IP Address—**A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

d) From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:

- **Any—**Any protocol (this is the default value)
- **TCP—**Transmission Control Protocol
- **UDP—**User Datagram Protocol
- **ICMP/ICMPv6—**Internet Control Message Protocol

Note ICMPv6 is only available for IPv6 ACL.

- **ESP—**IP Encapsulating Security Payload
- **AH—**Authentication Header
- **GRE—**Generic Routing Encapsulation
- **IP in IP—**Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP—**Ethernet-over-Internet Protocol
- **OSPF—**Open Shortest Path First
- **Other—**Any other Internet Assigned Numbers Authority (IANA) protocol

Note If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The controller can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

e) If you chose TCP or UDP in the previous step, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

Note Source and Destination ports based on the ACL type.

f) From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.

- **Any—**Any DSCP (this is the default value)
- **Specific—**A specific DSCP from 0 to 63, which you enter in the DSCP edit box

g) From the **Direction** drop-down list, choose one of these options to specify the direction of the traffic to which this ACL applies:

- **Any—**Any direction (this is the default value)
- **Inbound—**From the client
- **Outbound—**To the client

Note If you are planning to apply this ACL to the controller CPU, the packet direction does not have any significance, it is always 'Any'.

h) From the **Action** drop-down list, choose Deny to cause this ACL to block packets or Permit to cause this ACL to allow packets. The default value is Deny.

i) Click **Apply** to commit your changes. The **Access Control Lists > Edit** page reappears, showing the rules for this ACL.
The **Deny Counters** fields shows the number of times that packets have matched the explicit deny ACL rule. The **Number of Hits** field shows the number of times that packets have matched an ACL rule. You must enable ACL counters on the Access Control Lists page to enable these fields.

Note If you want to edit a rule, click the sequence number of the desired rule to open the **Access Control Lists > Rules > Edit** page. If you want to delete a rule, hover your cursor over the blue drop-down arrow for the desired rule and choose **Remove**.

j) Repeat this procedure to add any additional rules for this ACL.

Step 9 Click **Save Configuration** to save your changes.

Step 10 Repeat this procedure to add any additional ACLs.

Applying an Access Control List to an Interface

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the name of the desired interface. The **Interfaces > Edit** page for that interface appears.

Step 3 Choose the desired ACL from the ACL Name drop-down list and click **Apply**. The default is None.

Note Only IPv4 ACL are supported as interface ACL.

Step 4 Click **Save Configuration** to save your changes.

Applying an Access Control List to the Controller CPU

Step 1 Choose **Security** > **Access Control Lists** > **CPU Access Control Lists** to open the CPU Access Control Lists page.

Step 2 Select the **Enable CPU ACL** check box to enable a designated ACL to control the IPv4 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.

Step 3 From the ACL Name drop-down list, choose the ACL that will control the IPv4 traffic to the controller CPU. None is the default value when the CPU ACL feature is disabled. If you choose None while the Enable CPU ACL check box is selected, an error message appears indicating that you must choose an ACL.

Note This parameter is available only if you have selected the CPU ACL Enable check box.

Note When CPU ACL is enabled, it is applicable to both wireless and wired traffic.

Step 4 Select the **Enable CPU IPv6 ACL** check box to enable a designated ACL to control the IPv6 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.

Note For CPU IPv6 ACL, along with permit rules for HTTP/Telnet, you must add a rule to allow ICMPv6 (NA/ND uses ICMPv6) for the CPU IPv6 ACLs to work.

Step 5 From the IPv6 ACL Name drop-down list, choose the ACL that will control the IPv6 traffic to the controller CPU. None is the default value when the CPU ACL feature is disabled. If you choose None while the Enable CPU IPv6 ACL check box is selected, an error message appears indicating that you must choose an ACL.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Applying an Access Control List to a WLAN

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 From the **Override Interface ACL** drop-down list, choose the IPv4 or IPv6 ACL that you want to apply to this WLAN. The ACL that you choose overrides any ACL that is configured for the interface. None is the default value.

Note To support centralized access control through AAA server such as ISE or ACS, IPv6 ACL must be configured on the controller and the WLAN must be configured with AAA override enabled feature.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Applying a Preauthentication Access Control List to a WLAN

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 Select the **Web Policy** check box.

Step 5 From the **Preauthentication ACL** drop-down list, choose the desired ACL and click **Apply**. None is the default value.

Step 6 Click **Save Configuration** to save your changes.

Configuring and Applying Access Control Lists (CLI)

Configuring Access Control Lists

Step 1 See all of the ACLs that are configured on the controller by entering this command:
show [**ipv6**] **acl summary**

Step 2 See detailed information for a particular ACL by entering this command:
show [**ipv6**] **acl detailed** *acl_name*
The Counter text box increments each time a packet matches an ACL rule, and the DenyCounter text box increments each time a packet does not match any of the rules.

Note If a traffic/request is allowed from the controller by a permit rule, then the response to the traffic/request in the opposite direction also is allowed and cannot be blocked by a deny rule in the ACL.

Step 3 Enable or disable ACL counters for your controller by entering this command:
config acl counter {**start** | **stop**}

Note If you want to clear the current counters for an ACL, enter the **clear acl counters** *acl_name command.*

Step 4 Add a new ACL by entering this command:
config [ipv6] **acl create** *acl_name*.
You can enter up to 32 alphanumeric characters for the *acl_name* parameter.

Note When you try to create an interface name with space, the controller CLI does not create an interface. For example, if you want to create an interface name int 3, the CLI will not create this since there is a space between int and 3. If you want to use int 3 as the interface name, you need to enclose within single quotes like ‘int 3’.

Step 5 Add a rule for an ACL by entering this command:
config [ipv6] acl rule add acl_name rule_index

Step 6 Configure an ACL rule by entering **config [ipv6] acl rule** command:

Step 7 Save your settings by entering this command:
save config

Note To delete an ACL, enter the **config** [**ipv6**] **acl delete** *acl_name* command. To delete an ACL rule, enter the **config** [**ipv6**] **acl rule delete** *acl_name rule_index* command.

Applying Access Control Lists

Step 1 Perform the following to apply an IPv4 ACL:

- To apply an ACL to the IPv4 data path, enter this command:

  config acl apply acl_name

- To apply an ACL to the controller CPU to restrict the IPv4 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:
  config acl cpu acl_name {wired | wireless | both}

  Note To see the ACL that is applied to the controller CPU, enter the **show acl cpu command**. To remove the ACL that is applied to the controller CPU, enter the **config acl cpu none** command.

  Note For 2504 and 4400 series WLC, the CPU ACL cannot be used to control the CAPWAP traffic. Use the access-list on the network to control CAPWAP traffic.

Step 2 Perform the following to apply an IPv6 ACL:

- To apply an ACL to an IPv6 data path, enter this command:

  config ipv6 acl apply name

- To apply an ACL to the controller CPU to restrict the IPv6 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:
  config ipv6 acl cpu {name|none}

Step 3 To apply an ACL to a WLAN, enter this command:

- **config wlan acl** *wlan_id acl_name*

  Note To see the ACL that is applied to a WLAN, enter the **show wlan** *wlan_id command*. To remove the ACL that is applied to a WLAN, enter the **config wlan acl** *wlan_id* **none** command.

Step 4 To apply a pre-authentication ACL to a WLAN, enter this command:

- **config wlan security web-auth acl** *wlan_id acl_name*

Step 5 Save your changes by entering this command:
save config

Configuring Layer 2 Access Control Lists

Information About Configuring Layer 2 Access Control Lists

You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.

In a mobility scenario, the mobility anchor configuration is applicable.

The following traffic is not blocked:

- Wireless traffic for wireless clients:
  - 802.1X
  - Inter-Access Point Protocol
  - 802.11
  - Cisco Discovery Protocol
- Traffic from a distributed system:
  - Broadcast
  - Multicast
  - IPv6 Neighbor Discovery Protocol (NDP)
  - Address Resolution Protocol (ARP) and Gratuitous ARP Protection (GARP)
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)

Layer 2 ACL Mapping to WLAN

If you map a Layer 2 ACL to a WLAN, the Layer 2 ACL rules that you configure apply to all the clients that are associated with that WLAN.

When you map a Layer 2 ACL to a centrally switched WLAN, the rule to pass traffic based on the Ethertype is determined by Fast-Path for every client that is associated with the WLAN. Fast-Path looks into the Ethernet headers associated with the packets and forwards the packets whose Ethertype matches with the one that is configured for the ACL.

When you map a Layer 2 ACL to a locally switched WLAN, the rule to pass traffic based on the Ethertype is determined by the forwarding plane of the AP for every client that is associated with the WLAN. The AP forwarding plane looks into the Ethernet headers associated with the packets and forwards or denies the packets based on the action whose Ethertype matches with the one that is configured for the ACL.

Note WLC devices configured to preform Central Switching and Centralized Authentication displays the name of the Layer-2 ACL being applied to roaming users incorrectly. The situation occurs when an authorized device preforms a Layer-3 roam from the anchor controller to a foreign controller. After roaming, if an administrator issues the **show acl layer2 summary** command on the CLI of the foreign controller the incorrect information is displayed. It is expected that the ACL applied by the anchor will follow the authenticated client as it roams from controller to controller.

Restrictions on Layer 2 Access Control Lists

- You can create a maximum of 16 rules for a Layer 2 ACL.
- AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs.

- You can create a maximum of 64 Layer 2 ACLs on a controller.
- A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.
- Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

Configuring Layer 2 Access Control Lists (CLI)

- **config acl layer2** {**create** | **delete**} *acl-name*—Creates or deletes a Layer 2 ACL.
- **config acl layer2 apply** *acl-name*—Applies a Layer 2 ACL to a data path.
- **config acl layer2 rule** {**add** | **delete**} *acl-rule-name index*—Creates or deletes a Layer 2 ACL rule.
- **config acl layer2 rule change index** *acl-rule-name old-index new-index*—Changes the index of a Layer 2 ACL rule.
- **config acl layer2 rule action** *acl-rule-name index* {*permit* | *deny*}—Configures an action for a rule.
- **config acl layer2 rule etherType** *name index ether-type-number-in-hex ether-type-mask-in-hex*—Configures the destination IP address and netmask for a rule.
- **config acl layer2 rule swap index** *acl-rule-name index-1 index-2*—Swaps the index values of two rules.
- **config acl counter** {**start** | **stop**}—Starts or stops the ACL counter. This command is applicable for all types of ACLs. In an HA environment, the counters are not synchronized between the active and standby controllers.
- **show acl layer2 summary**—Shows a summary of the Layer 2 ACL profiles.
- **show acl layer2 detailed** *acl-name*—Shows a detailed description of the Layer 2 ACL profile specified.
- **show client detail** *client-mac-addr*—Shows the Layer 2 ACL rule that is applied to the client.

Mapping of Layer 2 ACLs with WLANs (CLI)

This is applicable to centrally switched WLANs and locally switched WLANs without FlexConnect access points.

- **config wlan layer2 acl** *wlan-id acl-name*—Maps a Layer 2 ACL to a centrally switched WLAN.
- **config wlan layer2 acl** *wlan-id none*—Clears the Layer 2 ACLs mapped to a WLAN.
- **show wlan** *wlan-id*—Shows the status of a Layer 2 ACL that is mapped to a WLAN.

Mapping of Layer 2 ACLs with Locally Switched WLANs Using FlexConnect Access Points (CLI)

This is applicable to locally switched WLANs that have FlexConnect access points.

- **config ap flexconnect wlan l2acl add** *wlan-id ap-name acl-name*—Maps a Layer 2 ACL to a locally switched WLAN.

- **config ap flexconnect wlan l2acl** *delete wlan-id ap-name*—Deletes the mapping.
- **show ap config general** *ap-name*—Shows the details of the mapping.

Configuring Layer 2 Access Control Lists (GUI)

Step 1 Choose **Security** > **Access Control Lists** > **Layer2 ACLs** to open the Layer2 Access Control Lists page.

Step 2 Add a new ACL by clicking **New**. The Layer2 Access Control Lists > New page appears.

Step 3 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**. When the Layer2 Access Control Lists page reappears, click the name of the new ACL.

Step 5 When the Layer2 Access Control Lists > Edit page appears, click **Add New Rule**. The Layer2 Access Control Lists > Rules > New page appears.

Step 6 Configure a rule for this ACL as follows:

a) The controller supports up to 16 rules for each ACL. These rules are listed in order from 1 to 16. In the Sequence text box, enter a value (between 1 and 16) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 through 4 are already defined and you add rule 15, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b) From the Ether Type drop-down list, choose any option from the following Ether type:

- AppleTalk Address Resolution Protocol
- VLAN-tagged Frame & Short Path Bridging
- IPX (0x8137)
- IPX (0x8138)
- QNS Qnet
- Internet Protocol Version 6
- Ethernet Flow Control
- Slow Protocol
- CobraNet
- MPLS Unicast
- MPLS Multicast
- PPPoE Discovery Stage
- PPPoE Session Stage
- Jumbo Frames
- HomePlug 1.0 MME
- EAP over LAN

- PROFINET over Protocol
- HyperSCSI
- ATA over Ethernet
- EtherCAT Protocol

Note You can select any predefined Ether Types from the Ether Type drop-down list or enter your own Ether type value using the custom option from the Ether Type drop-down list.

c) From the **Action** drop-down list, choose Deny to cause this ACL to block packets or Permit to cause this ACL to allow packets. The default value is Deny.
d) Click **Apply** to commit your changes. The Layer2 Access Control Lists > Edit page reappears, showing the rules for this ACL.
e) Repeat this procedure to add any additional rules for this ACL.

Step 7 Click **Save Configuration** to save your changes.
Step 8 Repeat this procedure to add any additional ACLs.

Applying a Layer2 Access Control List to a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.
Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.
Step 4 From the **Layer2 ACL** drop-down list, choose the ACL you have created.
Step 5 Click **Apply**.
Step 6 Click **Save Configuration**.

Applying a Layer2 Access Control List to an AP on a WLAN (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the desired access point to open the **All APs > Details** page.

Step 3 On the **All APs > Details** page, click the **FlexConnect** tab.

Step 4 From the **PreAuthentication Access Control Lists** area, click the **Layer2 ACLs** link to open the **ACL Mappings** page.

Step 5 From the **Layer2 ACL** drop-down list in the WLAN ACL Mapping area, choose the ACL you have created and click **Add**.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring DNS-based Access Control Lists

Information About DNS-based Access Control Lists

The DNS-based ACLs are used for client devices such as Apple and Android devices. When using these devices, you can set pre-authentication ACLs on the Cisco WLC to determine where devices have the right to go.

To enable DNS-based ACLs on the Cisco WLC, you need to configure the allowed URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The Cisco WLC is configured with the ACL name and that is returned by the AAA server for pre-authentication ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the Cisco WLC, the CAPWAP payload is sent to the AP enabling DNS snooping on the client and the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the Cisco WLC as a CAPWAP payload. The Cisco WLC adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

In Release 8.0, support was added for DNS-based ACL with local web authentication.

Restrictions on DNS-based Access Control Lists

- Maximum of 10 URLs can be allowed for an access control list.

- On the Cisco WLC, 20 IP addresses are allowed for one client.
- Local authentication is not supported for FlexConnect APs.
- DNS-based ACLs are not supported on FlexConnect APs with Local Switching.
- DNS-based ACLs are not supported on Cisco 1130 and 1240 series access points.
- Authentication traffic has to go through the Cisco WLC for this feature to be supported, even if DNS-based ACL is local to the AP.
- If a client is anchored, be it auto-anchor or after roaming, DNS-based ACLs do not work.

Configuring DNS-based Access Control Lists (CLI)

Step 1 Specifies to create ACL. You can enter an IPv4 ACL name up to 32 alphanumeric characters.
config acl create *name*

Example:
```
(Cisco Controller) >> config acl create android
```

Step 2 Specifies to add a new URL domain for the access control list. URL domain name should be given in a valid format, for example, Cisco.com, bbc.in, or play.google.com. The hostname comparison is a sub string matched (wildcard based). You must use the ACL name that you have created already.
config acl url-domain add *domain-name acl-name*

Example:
```
(Cisco Controller) >> config acl url-domain add cisco.com android
(Cisco Controller) >> config acl url-domain add play.google.com android
```

Step 3 Specifies to delete an existing URL domain for the access control list.
config acl url-domain delete *domain-name acl-name*

Example:
```
(Cisco Controller) >> config acl url-domain delete cisco.com android
```

Step 4 Specifies to apply the ACL.
config acl apply *acl-name*

Example:
```
(Cisco Controller) >> config acl apply android
```

Step 5 Displays DNS-based ACL information by entering this command:
show acl summary

Example:
```
(Cisco Controller) >> show acl summary

ACL Counter Status              Disabled
-----------------------------------------
IPv4 ACL Name                    Applied
------------------------------- -------
android                          No
```

```
StoreACL                          Yes
----------------------------------------
IPv6 ACL Name                     Applied
--------------------------------- -------
```

Step 6 Displays detailed DNS-based ACL information by entering this command:
show acl detailed *acl-name*

Example:

```
(Cisco Controller) >> show acl detailed android
o rules are configured for this ACL.
DenyCounter : 0
URLs configured in this ACL
---------------------------
*.play.google.com
*.store.google.com
```

Step 7 Displays the IP addresses per client learned through DNS snooping (DNS-based ACL) by entering this command:
show client detail *mac-address*

Example:

```
(Cisco Controller) >> show client detail mac-address
```

Step 8 Enables debugging of information related to DNS-based ACL.
debug aaa events enable

Example:

```
(Cisco Controller) >> debug aaa events enable
```

Configuring DNS-based Access Control Lists (GUI)

Step 1 Choose **Security** > **Access Control Lists** > **Access Control Lists** to open the Access Control Lists page.

Step 2 If you want to see if packets are hitting any of the ACLs configured on your controller, select the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unselected, which is the default value. This feature is useful when troubleshooting your system.

Note If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.

Step 3 Add a new ACL by clicking **New**. The Access Control Lists > New page appears.

Step 4 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Select the ACL type as IPv4.

Step 6 Click **Apply**.

Step 7 When the **Access Control Lists** page reappears, click the name of the new ACL. The ACLs have no IP rules. Hover your cursor over the blue drop-down arrow, choose **Add-Remove URL** from the drop-down list to open the URL List page.

Step 8 To add a new URL domain for an ACL, enter the new URL domain for the access control list in the **URL String Name** text box. The URL domain name should be given in a valid format, for example, Cisco.com, bbc.in, or play.google.com.

Step 9 To delete an URL domain, hover your cursor over the blue drop-down arrow under the URL Name you want to delete, and select **Delete**.

Configuring URL Filtering

Information About URL Filtering

URL filtering feature allows you to control access to internet websites. It does so by permitting or denying access to specific websites based on information contained in a URL access control list (ACL). The URL filtering then restricts access based on the ACL list.

Using location based filtering, APs are grouped under various AP groups and WLAN profiles separate trusted and non-trusted clients within the same SSID. This forces re-authentication and new VLAN when a trusted client moves to a non-trusted AP or vice-versa.

The Wireless Controller (WLC) supports up to 64 ACLs. These ACLs are configured to either permit or deny requests, and can be associated with different interfaces (ex: WLAN, LAN), thus increasing effective filtering. Policies can be implemented locally on a WLAN or an AP group that is different from the applied global policy.

The policy priority order is:

1. Policy
2. Interface
3. WLAN

Note Default settings is to deny requests where the request URL does not match the applied ACL.

The number of rules (URLs) supported in each ACL varies for different WLCs:

- Cisco 5508 WLC, WiSM2 support 64 rules in one ACL.
- Cisco 5520, 8510, 8540 WLCs support 100 rules in one ACL.

Restrictions for URL Filtering

- Not supported on Cisco 2504 WLCs, vWLC, and Mobility Express.
- This feature is supported only on WLAN Central Switching and not Local switching.
- Not supported in Flex mode with local switching.
- Currently not supported
  - Wildcard URLs (ex: www.uresour*loc.com).
  - Sub-URL (ex: www.uresour*loc.com/support).
  - Sub-Domain (ex: reach.url.com or sub1.url.com)
- URL name is limited to 32 characters in length.
- No AVC Profile for the matched URLs. ACL Actions support for the Matched URLs.
- White list and Black list can be created using the "*" implicit rule in the ACL to permit or deny requests respectively.
- Only HTTP URLs are supported.
- Radius server returning URL filtering ACL name is not supported.
- ACL may fail to filter in the following situations:
  - URL is across fragmented packets.
  - IP packets are fragmented.
  - Direct IP address or proxy setup used instead of URL.

Configuring URL Filtering (GUI)

Configuring Access Control Lists (GUI)

To create or delete access control lists in an WLAN.

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page.

Step 2 Select the **Enable URL Acl** check box to enable the URL ACL feature.

Step 3 Add a new ACL by clicking **New**. The **URL Access Control Lists** > **New** page appears.
In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

- Repeat this procedure to add any additional URL ACLs.
- To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

Note If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.

Configuring an URL ACL List (GUI)

Configuring rules in an URL ACL List.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page	
Step 2	Choose the URL ACL.	**URL Access Control Lists** > **Edit**page appears.
Step 3	Choose **Add New Rule**.	
Step 4	Configure a rule for this ACL from the drop-down menu.	• Rule Index—range between 1 and 100. • URL—enter the URL address. • Action—select Permit or Deny.
Step 5	Click **Apply**.	Repeat this procedure to add any additional rules. **Note** To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: Enter the URL as website.com:8080 and apply permit action.

Applying a URL Filtering Access Control List Globally (GUI)

Applying the URL ACL to the entire network.

Step 1 Choose **Security** > **Local Policies** to open the local policy page.

Step 2 Choose the desired policy.
Policy > **Edit**page appears.

Step 3 Enter the **Match Role String** in the text box.

Step 4 Select the URL ACL from the **URL ACL** drop-down list.

Step 5 Click **Apply**.

Note The **Match Role String** name should match the role name in Cisco AV pair.

Applying a URL Filtering Access Control List to an Interface (GUI)

Applying the URL ACL to an interface in the network.

Step 1 Choose **Controller** > **Interfaces** to open the interface page.

Step 2 Choose the desired interface.
The interface page for the selected interface appears.

Step 3 Select the URL ACL from the **URL ACL** drop-down list.

Step 4 Click **Apply**.

Applying a URL Filtering Access Control List for a WLAN (GUI)

Applying the URL ACL to a WLAN in the network.

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.
The **WLANs** > **Edit** page appears.

Step 3 Choose the **Advanced** tab.

Step 4 From the **URL ACL** drop-down list, choose the ACL that you want to apply to this WLAN.

Step 5 Click **Apply**.

Mapping the policy to a WLAN (GUI)

Mapping the policy to a WLAN in the network.

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.
The **WLANs** > **Edit** page appears.

Step 3 Choose the **Policy-Mapping** tab.

1. Enter the Priority Index value.

2 Choose the local policy from the **Local Policy** drop-down list.

3 Click **Add**.

Step 4 Click **Apply**.

To delete a Policy-Mapping in a WLAN (GUI)

This procedure helps delete the policy-mapping in a WLAN.

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.
The **WLANs** > **Edit** page appears.

Step 3 Hover the mouse cursor over the blue drop-down arrow for that local policy

Step 4 Choose **Remove**
The confirmation box appears.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Mapping the policy to an AP Group (GUI)

Mapping the policy to an AP Group in the network.

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Choose **Advanced** > **AP Groups**.

Step 3 Choose the **AP Group**.
The **AP Groups** > **Edit** page appears.

Step 4 Choose the **WLANs** tab.

Step 5 Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select **Policy-Mapping**.

Step 6 In the **AP Group** > **Policy** > **Mappings** page.

1 Enter the Priority Index value.

2 Choose the local policy from the **Local Policy** drop-down list.

3 Click **Add**.

Step 7 Click **Apply**.
The WLAN and AP Group are Local Role based policies.

Configuring URL Filtering (CLI)

Configuring URL Filtering (CLI)

Step 1 Configure the URL based Filtering feature by entering this command:
config acl url-acl {**enabled | disable**}

Step 2 Create or delete a URL ACL by entering this command:
config acl url-acl{ **create | delete**} *id-token*

Step 3 Apply the URL ACL to the data path by entering this command:
config acl url-acl apply*acl-name*

Step 4 Configure an acl to an interface by entering this command:
config interface url-acl *interface-name acl-name*

Step 5 Configure an acl to a WLAN by entering this command:
config wlan url-acl *wlan-id acl-name*

Configuring Access Control List Rules (CLI)

Step 1 Create or delete a ACL by entering this command:
config acl url-acl rule{ **add | delete**} *acl-name index*

Step 2 Configure the URL address in a valid format (example: www.cisco.com) by entering this command:
config acl url-acl rule url*acl-name index url-name*

Step 3 Configure the action of the rule by entering this command:
config acl url-acl rule action *acl-name index*{ **permit | deny**}

Note To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: enter the URL as website.com:8080 and apply permit action.

Applying Local Policy (CLI)

Step 1 Create or delete a local profiling policy by entering this command:

config policy *policy-name*{**create | delete**}

Step 2 Configure a match type to a policy by entering this command:
config policy *policy-name* **match role** {**role-name| none**}

Step 3 Configure an action to a policy by entering this command:
config policy *policy-name* **action url-acl** {**enable | disable**} *acl-name*

Step 4 Activate a local policy to a WLAN by entering this command:
config wlan policy add *priority-index policy-name wlan-id*

Step 5 Add or delete a local policy in an AP group in a WLAN by entering this command:
config wlan apgroup policy {**add | delete**} *priority-index policy-name ap-group-name wlan-id*

Viewing URL Filtering (CLI)

- View ACL summary by entering this command:
  show acl url-acl summary
- View detailed URL ACL profile information by entering this command:
  show acl url-acl detailed *acl-name*
- View the details of a policy by entering this command:
  show policy {**summary**|*policy-name*}
- View client details by MAC address by entering this command:
  show client detail *mac-address*
- View the WLAN configuration details by entering this command:
  show wlan *wlan-id*
- View the interface details by entering this command:
  show interface detailed *interface-name*
- Clear the counters by entering this command:
  clear url-acl-counters

Troubleshooting URL Filtering (CLI)

You can troubleshoot the URL Filtering feature by entering these commands:

- **debug fastpath dump urlacldb** *aclid ruleindex dataplane*
- **debug fastpath dump stats** *dataplane*
  The dataplane options available are 0, 1, All.
- **debug fastpath dump scbdb**